

REMARKS

This is in response to the Office Action mailed on September 13, 2004, and the references cited therewith.

Claims 1, 17, 34, and 35 are amended; as a result, claims 1-37 are now pending in this application.

§102 Rejection of the Claims

Claim 34 was rejected under 35 USC § 102(b) as being anticipated by Demers *et al.* (U.S. 5,857,023). It is of course fundamental that in order to sustain an anticipation rejection that each and every element in the rejected claim must be taught or suggested in the cited reference.

Applicant's amended claim 34 now positively recites a signal having an entity identifier, where that entity identifier includes an encoded version of an entity name, a secret value, and a random number. The arrangement of this information is further defined within the amended claim 34, such that the three pieces of information are first bitwise concatenated with one another to produce an intermediate result. The intermediate result is hashed to produce a hash result, and the hash result is further bitwise concatenated with the random number a second time to produce the entity identifier embodied in the signal.

As support for this amendment, and by way of example only, the Examiner's attention is directed to the original filed specification page 19 beginning at the last paragraph and continuing onto page 20 in the first paragraph.

Demers fails to teach the arrangement of the information that forms the entity identifier in the manners taught and positively recited in Applicant's amended claim 34. Specifically, the nonce in Demers is not *concatenated* twice in forming the hash. *Emphasis added.* Demers, col. 9, lines 1-11. Accordingly, the rejection with respect to claim 34 should be withdrawn.

§103 Rejection of the Claims

Claims 1-5, 8, 13, 15-21, 25, 27-30 and 35 were rejected under 35 USC § 103(a) as being not patentable over Hoke *et al.* (U.S. 6,701,437) in view of Schneier (Applied Cryptography). To sustain an obviousness rejection each and every step or element in the rejected claims must be taught or suggested in the proposed combinations of the references cited.

Hoke is directed to Virtual Private Network (VPN) implementations. Thus, the Applicant would like to point out that in Hoke VPN units are affixed to front and back end communications occurring between clients. The participating clients are connected within the VPN, if a particular client is not connected within the VPN, then a VPN receiving unit issues a challenge to the non connected client for purposes of authenticating that client. Hoke, col. 8, lines 52-65.

Thus, at the outset, Applicant respectfully disagrees with the Examiner's conclusion that Hoke teaches: "connecting an originally-connected entity to an original endpoint," which is positively recited in Applicant's original and non-amended versions of the independent claims. This is so, because in Hoke a client is either connected within the VPN in which case no connecting is needed; or a client is not connected at all within the VPN in which case it could not have been originally connected.

Independent claims 1, 17, and 35 have been amended. These amendments now positively recite that the entity identifier or connection identifier serves as an index into a data structure for acquiring cryptographic context information or is linked to the cryptographic context information. Hoke fails to teach these limitations.

Specifically, Applicant's invention is capable of facilitating connections between entities and end-points even after connections have been lost. This is possible because the entity identifier or connection identifiers provide a link to the needed cryptographic context information for a connection to take place.

This is not achievable in Hoke because in Hoke once a connection is lost, the client has to be reconnected for authentication information. The authentication information is not retained and available in Hoke; but it is available via the cryptographic context that is maintained and managed with Applicant's invention. The encrypted entity identifier or connection identifier serves as a mechanism for acquiring portable cryptographic context information that can be used to facilitate a variety of connections between trusted entities that hold the secret for decrypting the identifiers and that know how to use the decrypted identifier's components for purposes of acquiring the needed cryptographic context information.

Accordingly, Hoke fails to teach an entity identifier or a connection identifier that is used as an index or link to specific cryptographic context information. Therefore, Applicant respectfully requests that the rejections with respect to the independent claims 1, 17, and 35 be

withdrawn and the claims allowed, because the missing teachings of Hoke are also not present in Schneier.

Claims 6, 9-12, 14, 22-24, 26, 31-33 and 36-37 were rejected under 35 USC § 103(a) as being not patentable over Hoke *et al.* and Schneier as applied to claim 1, and further in view of Demers *et al.* Claims 6, 9-12, and 14 are dependent from amended independent claim 1. Claims 22-24, 26, and 31-33 are dependent from amended independent claim 17. Claims 36 and 37 are dependent from amended independent claim 35. Therefore, for the remarks presented herein and above with respect to amended claims 1, 17, and 35, the rejections of claims 6, 9-12, 14, 22-24, 26, 31-33, and 36-37 should be withdrawn and these claims allowed. Applicant respectfully requests an indication of the same.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (513) 942-0224 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

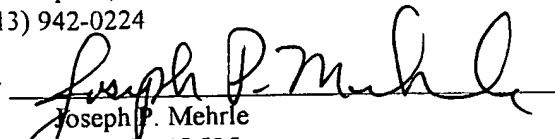
HILARIE K. ORMAN

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(513) 942-0224

Date 12-13-04

By


Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 13th day of December, 2004.

Peter Rebuffoni
Name


Signature